Math 3032: Feb 2, 2023

Next week: LSC C202.

Today: some ideals in $R[x]$

Last time: Given any ring R, we constructed a new ring $R[x]$ of polynomials w/ coefs in R in one variable.

$R \subset R[x]$ a subring of "constant polys"

↳ not literally true: an elt of $R[x]$ we defined to be a sequence in R, infinitely long, eventually zero

not literally true that $\mathbb{N} \subset \mathbb{Z}$.

$\mathbb{N} = \{ \underset{0}{\emptyset}, \underset{1}{\{\emptyset\}}, \underset{2}{\{\emptyset, \{\emptyset\}\}}, \dots \}$

pairs (a,b) "a-b" only care about difference. $(a,b) \sim (a+1, b+1)$

E.g: $\mathbb{Q} \rightsquigarrow \mathbb{Q}[x] \rightsquigarrow \mathbb{Q}[x,y] \hookrightarrow \mathbb{Q}[x,y,z] \hookrightarrow$

$\uparrow$ $\qquad$ $\uparrow$ 11

R $\qquad$ $\left\{ \sum_{i=0} a_i x^i, \; a_i \in \mathbb{Q} \right\}$

again a ring

Slightly nontrivial statement: "$\mathbb{Q}[x,y] = \mathbb{Q}[y,x]$".

I mean: $\exists$ unique iso $R[x,y] \to R[y,x]$

which is id on R and sends $x \mapsto x$, $y \mapsto y$.

polys in y whose coeffs are polys in x

polys in x whose coeffs are polys in y.

E.g. $\mathbb{Q}[x,y]$ $\quad \hom(\mathbb{Q}[x,y], S) = \hom(\mathbb{Q}[x], S) \times S = \hom(\mathbb{Q}, S) \times S \times S.$

$\ni$

$a_0 + a_1 y + a_2 y^2$

w/ $a_i \in \mathbb{Q}[x]$

$\mathbb{Q}[y,x]$ ← use this s.

$\ni$

$2 + (1+3y^2)x + (4y^2)x^2 + (7y)x^3.$

e.g.

$(2+x) + (7x^3)y + (3x+4x^2)y^2$

↔

proof idea: we argued in general that a map $\mathbb{Q}[x,y] \to ?$ is • coefs. • variables.

Content of "slightly nontrivial statement": you always do such a rearranging.

Rather clear, but does require polys have finite degree.

Another ring: power series. $R[\![x]\!]$ or $R[[x]]$

Defn: An elt of $R[\![x]\!]$ is an infinite sequence in R

$(a_0, a_1, \ldots) = "\sum a_i x^i"$ possibly never zero.

e.g. $1 + x + x^2 + x^3 + \cdots \in R[\![x]\!]$.

addition: $\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) = \sum_i (a_i + b_i) x^i$.

multiplication: $\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k$

Although power series are infinite, this is still finite.

Again true $R[\![x]\!][\![y]\!] = R[\![y]\!][\![x]\!]$

Other variations:

$R[x^{\pm 1}]$ rule 3: "polys" can have negative powers.

e.g. $x^{-1} + 1 + 2x + x^2$.

(sequences in both directions, eventually zero in both dirs).

$R(\!(x)\!)$ aka $R[x^{-1}, x]\!]$

infinite in the x^{pos}, eventually zero in the x^{neg} dir.

e.g. $x^{-1} + 1 + x + x^2 + x^3 + \cdots$

"$R[[x^{\pm 1}]]$" infinite power series in both directions.

This is not a ring.
It is an additive gp.

$$\sum_{i+j=k} a_i b_j$$

for fixed k
is an infinite sum.
So no mult
reasonable.

$$R(x)(y)$$
$$\neq R(y)(x).$$

A typical ideal in $\mathbb{Z}[x]$.

- principal ideals.

(x^2) ← all polys in $\mathbb{Z}[x]$

$\|$

$a_0 + a_1 x + a_2 x^2 + \cdots$

s.t. $a_0, a_1 = 0$.

(2)

↑

all polys w/ even coefs.

$\ni a_0 + a_1 x + a_2 x^2 + \cdots + b_0 + b_1 x + b_2 x^2 + \cdots$

s.t. $a_0, a_1 = 0$, $a_{\geq 2}$ arbitrary, all b_i's are even.

$(x^2, 2) =$ polys $a_0 + a_1 x + a_2 x^2 + \cdots$

s.t. a_0, a_1 are even.

rest of coefs are arbitrary.

aka $(x^2) + (2)$

$\mathbb{Z}[x]/(x^2)$ = polys modulo adding anything in (x^2).

as a set, elts are $a_0 + a_1 x$.

as an ab. gp, this is $\mathbb{Z}^2$.

$(a_0 + a_1 x)(b_0 + b_1 x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \cancel{a_1 b_1 x^2}$

$\mathbb{Z}[x]/(2) = (\mathbb{Z}/2)[x] = \mathbb{Z}_2[x]$.

$\mathbb{Z}[x]/(2, x^2)$

$$(2) \subseteq (2, x^2) \subseteq R = \mathbb{Z}[x].$$

so corresponding to $(2, x^2)$, there is an ideal $J \subseteq R/(2) = \mathbb{Z}_2[x]$.

and $$\frac{R/(2)}{J} = R/(2, x^2)$$

who is J? $J = \frac{(2, x^2)}{(2)}$.

$\{a_0 + a_1 x : a_0, a_1 \in \mathbb{Z}_2\}$

$(a_0 + a_1 x)(b_0 + b_1 x)$

$=$

$a_0 \cdot b_0 + (a_1 b_0 + a_0 b_1)x$

[mod 2]

work it out $\rightsquigarrow$ $J = (x^2) \subseteq \mathbb{Z}_2[x]$.

$\mathbb{Z}[x]/(2, x^2) = \mathbb{Z}_2[x]/(x^2)$

$$(x^2) \subseteq (2, x^2) \subseteq R = \mathbb{Z}[x].$$

so corresponding to $(2, x^2)$, there is an ideal $J \subseteq R/(x^2) = \mathbb{Z}[x]/x^2$

and $$\frac{R/(x)}{J} = R/(2, x^2)$$

who is J? $J = \frac{(2, x^2)}{(x^2)}$.

$\{a_0 + a_1 x : a_0, a_1 \in \mathbb{Z}_2\}$

$(a_0 + a_1 x)(b_0 + b_1 x)$

$=$

$a_0 \cdot b_0 + (a_1 b_0 + a_0 b_1)x$

$\mod 2$

work it out $\rightsquigarrow$ $J = (2) \subseteq \mathbb{Z}[x]/(x^2)$

$\mathbb{Z}[x]/(2, x^2) = (\mathbb{Z}[x]/(x^2))/(2)$

If you allow infinite processes,
then every ring can be built by:

- $R \rightsquigarrow R[x]$
- quotienting by ideals.

---

many rings of interest arise
from finite iteration of these processes.

Is $(2, x^2) \subseteq \mathbb{Z}[x]$ principle?

Unpacked: $\exists$? a poly $p(x) \in (2, x^2)$

s.t. every elt of $(2, x^2)$ is a multiple of p?

$2 \in (2, x^2)$ $\quad$ $x^2 \in (2, x^2)$.

if p exists, since p divides 2, p is constant.

since it also divides x^2, $p = 1$.

But $1 \notin (2, x^2)$.

What does $\mathbb{Z}[i]$ ($i := \sqrt{-1}$) really mean?

or $\mathbb{Z}[\sqrt{-7}]$ or $\mathbb{Z}[\varphi]$ or ...

$\varphi = \frac{1+\sqrt{5}}{2}$

Defn:

$$\mathbb{Z}[\sqrt{-7}] := \frac{\mathbb{Z}[x]}{(x^2+7)}$$

Justification: Earlier, we defined $\mathbb{Z}[\sqrt{-7}]$ as a specific subring of $\mathbb{C}$.

There is definitely a hom

$$\mathbb{Z}[x] \longrightarrow \text{earlier meaning of } \mathbb{Z}[\sqrt{-7}] \subseteq \mathbb{C}.$$

why? value on coefs $\mathbb{Z}$ is forced ($1 \mapsto 1$)

we choose $x \mapsto \sqrt{-7}$.

↑ determines the homomorphism.

This hom is surjective.

So: $\mathbb{Z}[\sqrt{-7}] \cong \dfrac{\mathbb{Z}[x]}{\text{kernel}}$.

earlier meaning

what is kernel $\left(\mathbb{Z}[x] \longrightarrow \mathbb{Z}[\sqrt{-7}] \right)$? $= K$

$x \longmapsto \sqrt{-7}$

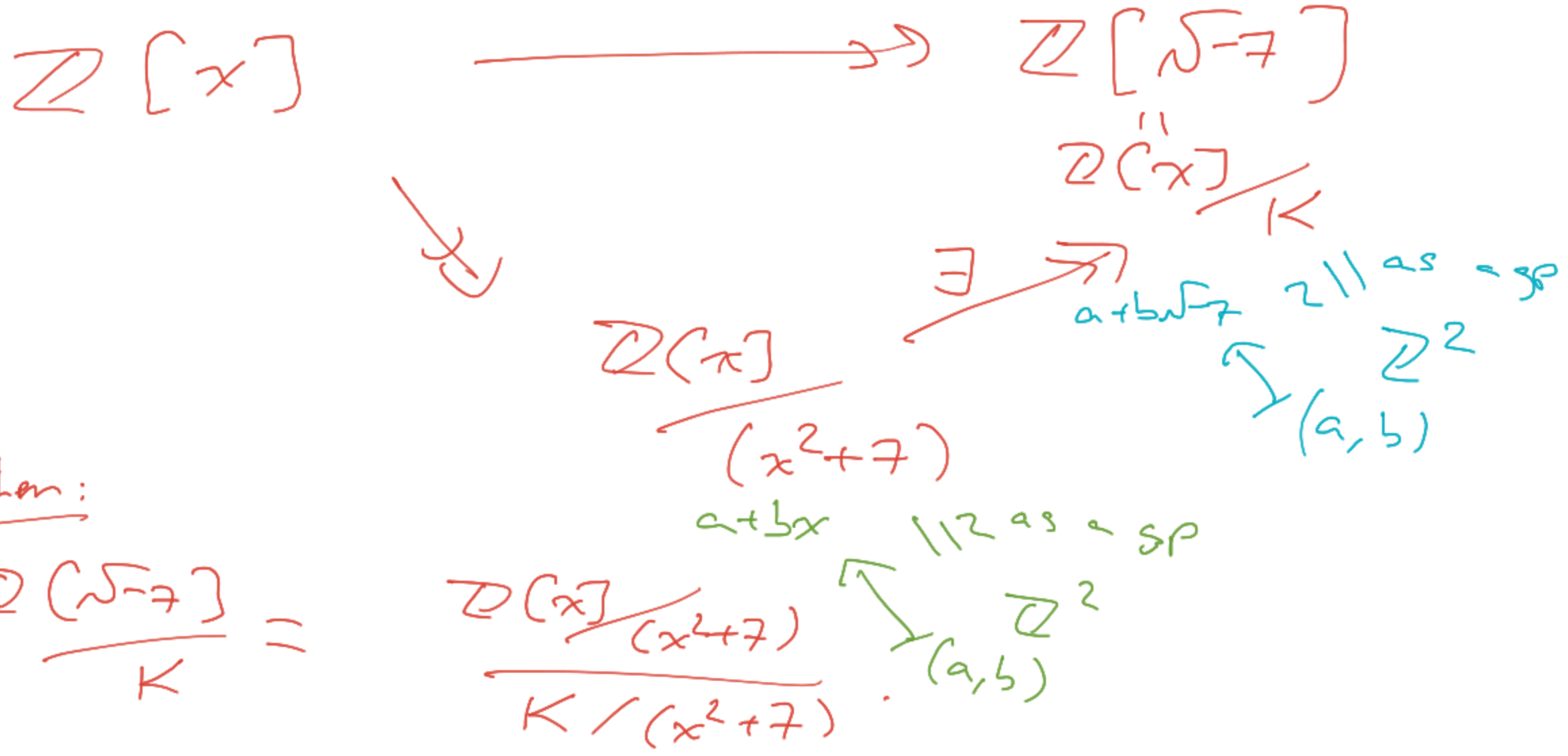
$=$

$\{$ polys w/ integer coefs which are zero at $x = \sqrt{-7}$ $\}$

$\cup$

$x^2 + 7$

$K \supseteq (x^2+7)$. WTS: They are equal.



Isomorphism:

$$\frac{\mathbb{Z}[\sqrt{-7}]}{K} \cong \frac{\mathbb{Z}[x]/(x^2+7)}{K/(x^2+7)}.$$

$$a + bx + cx^2 + \cdots + dx^7 \quad \text{in} \quad \mathbb{Z}[x]$$

$$\equiv c + bx + \text{things of degree} \leq ? \quad \text{mod} \ (x^2+7)$$

$$x^2 \equiv -7$$

$$x^3 \equiv -7x \quad \Big] \quad \text{i.e.} \quad x^3 = -7x + \text{something in ideal } (x^2+7).$$

$$x^4 \equiv -7x^2 \equiv 49$$

$$x^5 \equiv \cdots$$

Let R be a unital com ring.

In general:

A polynomial $p(x) \in R[x]$ is monic if its highest coef is 1.

↪ coef of deg = deg(p).

e.g. $x^3 + 3x + 7$ is monic.

$2x^3 + 3x + 7$ is not monic.

Prop: Suppose $p(x) \in R[x]$ is monic of deg n.

Then $$\frac{R[x]}{(p(x))} \underset{\text{as an ab gp}}{\cong} R^n$$

Specifically: basis is $\{1, x, x^2, \ldots, x^{n-1}\}$.

I'm claiming: (1) For polys of deg $< n$, if

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \equiv b_0 + \cdots + b_{n-1} x^{n-1} \mod p(x),$$

then $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2$, $\ldots$

(2) Every poly is $\equiv$ mod $p(x)$ to some poly of deg $< n$.

Pf:

(2) $x^n \overset{\text{⊛}}{\equiv} \underbrace{x^n - p(x)}_{\deg \le n-1} \mod p(x)$

deg ↑

so: if $N \ge n$, then $x^N \equiv$ something of $\deg \le N-1$.

(multiply ⊛ by x^{N-n}).

Iterate until $\deg \le n-1$, then stop.

(1) Equiv: If $r(x)$ has $\deg \le n-1$,

and $p(x)$ divides $r(x)$, then $r(x) = 0$.

$p(x) \cdot q(x) = r(x)$.

$p(x)$ = $x^n + \text{l.o.}$ $\quad$ $q(x)$ = $b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$

→ L.H.S = $b_m x^{n+m} + \text{l.o.}$

if $q(x) \neq 0$, then this has deg $n+m \ge n$. □